B-015

販売管理システムに対応する再利用可能な上位設計と UML/PROMELA 変換器を用いたモデル検査

Reusable Upstream Process Model and Model Checking using UML/PROMELA Converter that Corresponding to Sales Management Systems

高村 翔 †　　和崎 克己 ††
Sho Takamura　Katsumi Wasaki

1　はじめに

ソフトウェア開発の初期段階である上流工程の品質は，ソフトウェアの品質や開発期間を左右する．ソフトウェアの設計が正しいことを検証する手法の一つとしてモデル検査がある．モデル検査によるシステム検証は，検査対象を形式的に記述したモデルとして記述することが必要である．検証済みの誤りが無い設計を再利用することで，上流工程におけるコストを大幅に下げることができる．

モデル記述から，モデル検査器用のプロセスに変換する手法は広く研究されている．UML-PROMELA 変換器 [1][2] について著者らは種々の提案を行ってきた．本研究では POS システムなどを対象としている．POS システムは業態によって細かな点で違いがあるが，UML のクラス図の機能である継承を活用して様々な業態に対応できる設計の試作を行った．次に，モデル検査に必要となる PROMELA コードを UML から半自動生成できる，UML-PROMELA 変換器を用いたモデル検査とプロトタイピングにより，作成した設計の評価を試みた．

2　UML による上位設計

UML(Unified Modeling Language) は，OMG（Object Management Group）により管理されている仕様記述言語である [3]．グラフィカルな記述で抽象化したシステムのモデルを生成する汎用モデリング言語で，UML2.0 以降では 13 種類の図が定義されている．C++ や Java などオブジェクト指向言語によるシステム開発の増加から，実際のシステム開発でも広く用いられるようになった．UML はシステムの静的な性質である構造や，動的な性質の振る舞いを，文章ではなく準形式的な図として扱うことが可能であり，視認性が高い．実際の現場では，開発の初期段階である要求定義や設計で用いられ，本研究では UML を設計の場面で用いると想定している．

本研究で使用する UML は，構造を示す要素としてクラス図を使用する．また，各オブジェクトの動作をステートマシン図，通信をコミュニケーション図によって記述する．また，時系列に沿って，オブジェクトがどの様に振る舞うか，という仕様をシーケンス図で記述している．モデリングツールにはチェンジビジョン社の astah*[4] を用いる．astah*は，デザインエントリ全体を XML 形式のファイルとしてエクスポートする機能を有しており，後述するモデル検査に使用する．

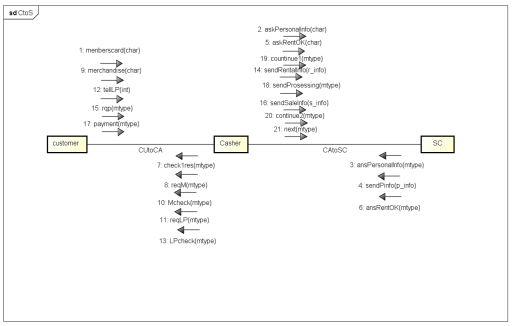

図 1　コミュニケーション図によるレンタル POS の記述例

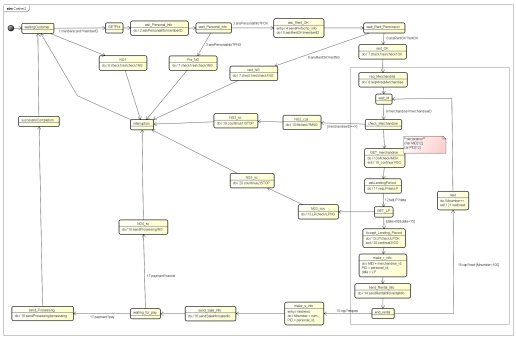

図 2　ステートマシン図によるレンタル POS 端末の記述例

3　再利用とモデル検査

ソフトウェア開発においてコードや設計情報などが再利用の対象として挙げられる．ライブラリやテンプレート，関数も再利用の例である．再利用を活用することの利点が開発期間の短縮である．コードや設計情報の一部を再利用することで，何もない状態よりも少ない期間で開発を進めることができる．今回は，UML で記述された上位設計を再利用することで，上流工程におけるコストの削減を目標としている．

ソフトウェア開発の初期段階である要求定義で，仕様に漏れや間違いがあると，誤りやバグに繋がる．ここでの誤りやバグは想定外の振る舞いや構造のことを指している．再利用を行う際，再利用元にバグや誤りが含まれている場合，再利用先にもそのバグや誤りが混入する．再利用する前に，設計に誤りやバグが含まれていないことを調査，検証する必要がある．設計から出力されるモデルが，形式仕様を満たすかどうかを検証できる手法として，モデル検査がある．モデル検査はシステムを網羅的に探査することで，システムの誤りやバグの発見が期待できる．モデル検査により検証されたシステムを再利用することで，誤りやバグがないシステムを短期間で開発することが可能だと考えられる．

† 信州大学大学院理工学系研究科，Graduate School of Science and Technology，Shinshu University.
†† 信州大学工学部，Faculty of Engineering，Shinshu University.

3.1　モデル検査とは

モデル検査はソフトウェアなどの仕様が正しく動くことを検証する手法である．検査対象となる仕様の振る舞いをプロセスとして記述し，検査器を用いて初期状態からとりうる状態を網羅的に調べ上げる．仕様に要求される性質は各ステップにおける表明，あるいは時相論理式などで記述し，性質に反している状態が発見された場合はエラーとして報告される．この手法は設計段階から適用することができるため，開発コストの削減に繋がることが期待される．

3.2　モデル検査器 SPIN

複数のモデル検査器が存在しているが，本研究ではモデル検査器 SPIN[5] を使用する．モデル検査器 SPIN(Simple Promela INterpreter) はベル研究所の G.J.Holzmann 氏によって提案されたモデル検査ツールである．検査する振る舞いであるモデルは，PROMELA(PROtocol/PROcess MEta LAnguage) という C 言語に近い専用の記述言語にて記述する．要求する性質の記述には，モデルに直接 assert 文を指示する方法の他に LTL 式 (Linear Temporal Logic) を用いる (図 3)．

4　UML-PROMELA 変換器を用いたモデル検査

UML-PROMELA 変換器は坂本ら [2] によって提案された変換器である．SPIN によるモデル検査は上述したように PROMELA でモデルを記述する必要があり，上位設計から手動でモデル化のコードを作成するコストがかかる．記述コストを削減する方法として，UML から PROMELA コードを出力するツールとして開発されたのが UML-PROMELA 変換器である．UML のコミュニケーション図とステートマシン図を用いてモデルを記述し，astah の XML 出力機能を用いてモデルの XML を出力する．出力した XML を変換器によって処理し，自動生成された PROMELA コードを得ることで，モデル検査を実行することができる．

4.1　UML 図の記述方法

コミュニケーション図では通信状態を記述する．各ノードの相互接続状況と，どのようなメッセージを流すのかを記述する．図 1 の記述では，レンタルビデオ店での様子を示している．Customer と Casher が CUtoCA，Casher と SC(Store Computer) が CAtoSC という通信経路で接続され，メッセージをやり取りしている．

ステートマシン図では通信機器がどのように振舞うのかを記述する．メッセージを受信した際の振る舞いなどを記述する．図 2 では，レンタルビデオ店における Casher の振る舞いを示している．顧客から個人情報や商材の情報が渡された際に，SC に問い合わせるなどの振る舞いを表した記述である．遷移に何も記述がなければ無条件で遷移が可能であり，記述がある場合は記述された条件を満たした場合のみ遷移する．

4.2　UML から PROMELA コードへの変換

本研究で開発している変換器は，Perl 言語で実装されており，astah*でエクスポートされた XML ファイルを基に変換を行う．PROMELA では，振る舞いをプロセスごとに記述し，プロセス間通信は，*chan* 型の変数で行う．自動変換後のプロセスと通信用チャネルは，コミュニケーション図で定義される．ライフライン (ノード) 毎にプロセスが生成され，各プロセスの振る舞いは関連付けられたステートマシン図から生成される．プロセスの振る舞いは関連付けられたステートマシン図から生成される．各プロセスは，どの状態であるかを保持する状態変数の値と，遷移条件を元に状態遷移を行う状態遷移モデルとして変換される．状態遷移モデルは，イベント受信によるイベント駆動遷移処理部と，イベントとは無関係に遷移する処理を記述する条件遷移処理部の 2 つで構成されている．

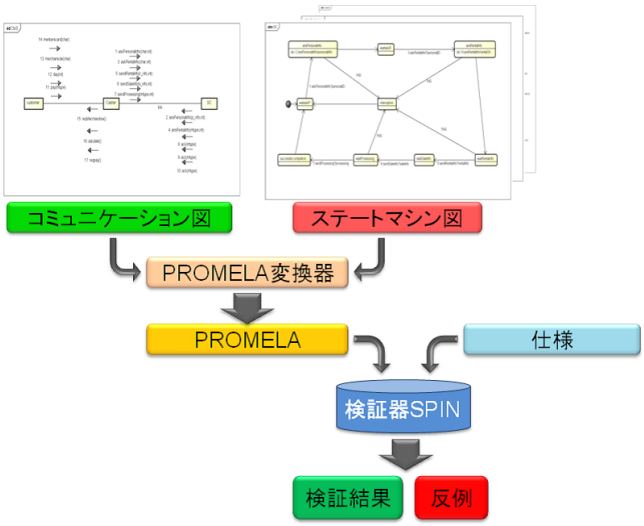

図 3　上位設計から UML-PROMELA 変換器による一貫したモデル検査環境

5　POS システムの上位設計

現在は，身近な例であり，再利用のしやすさの観点から POS(Pont Of Sales) システムをモデル化の対象としている．POS システムは販売時点情報管理システムのことで，販売した商品の名前，時間，個数などが記録される．販売実績情報を収集することで在庫や受発注管理が緻密に行える．POS システムはスーパーマーケットやコンビニ，レンタル店など多様な場所で使用されており，業務や企業により様々な種類の POS システムが存在している．しかし，殆どの POS システムは，会計という共通点が存在する．そこで共通点を軸に，異なる部分は UML の機能である継承を用いて，再利用性の高い上位設計の検討を行った．

5.1　POS システムのパターン

POS システムを使用する業務から，各々の業務の特徴を抽出し，そこから 3 種類のパターンに分類した．(1) 顧客への形ある商品を販売する業務を “物販パターン” とする．コンビニエンスストアやスーパーマーケットなどの POS システムがこれに該当する．商品の情報を読み込み，情報を元に顧客へ請求し，売り上げ情報を記録するという POS システムの基本となる流れである．(2) その場で料理や食料品，飲料などを飲食させ，その後会計する業態を “飲食パターン” とする．レストランや居酒屋などが該当する．物販との違いは，商品を提供

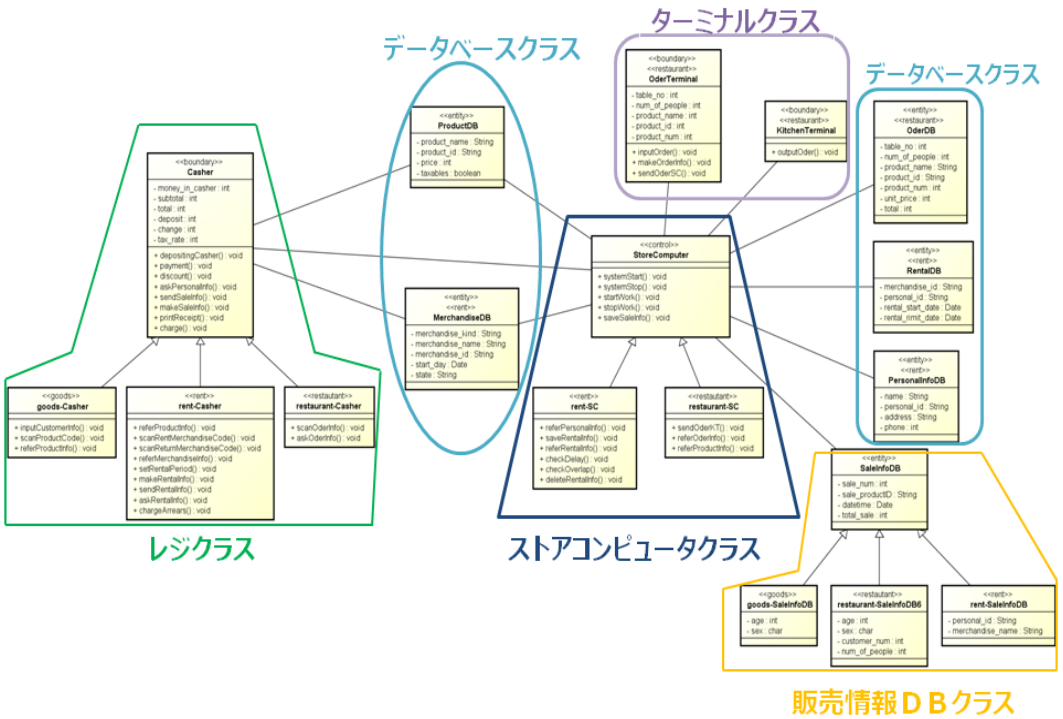

図 4　POS システムの上位設計：クラス図 (抜粋)

するフェーズと会計のフェーズが分かれている点である．(3) 代金と引き換えに，一定期間商品を貸し出す業態を “レンタルパターン” とする．レンタルビデオ店や貸衣装店が該当する．他の 2 つのパターンとの相違点として，個人情報の取り扱いや保存する機能を有することが挙げられる．それぞれ分類したパターンごとにクラス図，シーケンス図，コミュニケーション図，ステートマシン図の作成を行った．

5.2　継承を用いた上位設計クラス図の合成

5.1 節で挙げた 3 種類のパターン以外の業態についても，基本的な設計パターンの機能を多重継承することで，その上位設計が表現可能である．各々のパターンの UML を作成し，共通点を探し，クラス図に多くの共通点を見出した．どのパターンであってもキャッシュレジスタ (レジ) や，店舗内の情報を管理するストアコンピュータと販売情報を保存するためのデータベースが必須である．そこで，レジ，ストアコンピュータ，販売情報データベース (DB) はどのパターンでも必須のクラスとし，各々で必要となるクラスに関しては，クラスの継承を用いた表現で 3 パターンのクラス図を 1 つのクラス図へ合成した．これにより別のパターンのクラスやその一部を継承させることで，上位設計として対応可能な業態を増やすことができると考えられる．

3 種類のパターンには分類されないカラオケ店を例とする．カラオケ店は食事や飲料を注文しその場での飲食が可能であることから，飲食パターンに該当する．また，カラオケ店は顧客ごとに個室を貸していると考えると，レンタルパターンにも該当している．従って，カラオケ店の POS システムは飲食パターンとレンタルパターンの POS システムを組み合わせることで表現が可能であると考えられる．

6　モデル化した POS システムとモデル検査

5.1 節で説明した 3 種類のパターンにおいてそれぞれシーケンス図による仕様の記述 (図 5)，クラス図での構造の記述を行った．コミュニケーション図とステートマシン図で各オブジェクトの振る舞いの記述を行った．上述の通り，モデル検査には PROMELA で記述したモデルが必要であるが，UML-PROMELA 変換器を用いて上位設計データに基づいた半自動生成機能により，一貫したモデル検査が行える．

具体的には，変換器で PROMELA を出力するためには変換器独自の記述法によるステートマシン図，コミュニケーション図の定義が必要である．現在，レンタルパターンの貸し出しフェーズを対象として，変換器に沿った記述法での記述を行っている．作成したモデルをベースに，始めはストアコンピュータとストアコンピューターのみの通信によるシンプルなモデルから，段階的に様々な要素の追加，モデルの深化を行い記述を進めている．

今回の満たすべき仕様としては，どの様な顧客の振る舞いによってもシステムが停止しないことを目的としている．そのため，追加した顧客のモデル (図 6) には，顧客が手順を間違える，必要な手順をスキップする，という遷移が非決定的に選択される様にしている．また，故障などの障害により，データベースへの保存の失敗をカバーするために，トランザクション処理機能の追加も行っている．

7　まとめ

ソフトウェア開発初期段階の上流工程のコスト削減を目標とし，設計情報の再利用を提案する．そして POS システムに対して再利用性を考慮した設計の作成を行った．再利用を行うためには，再利用元に誤りやバグがないことが必要である．再利用に誤りやバグがな

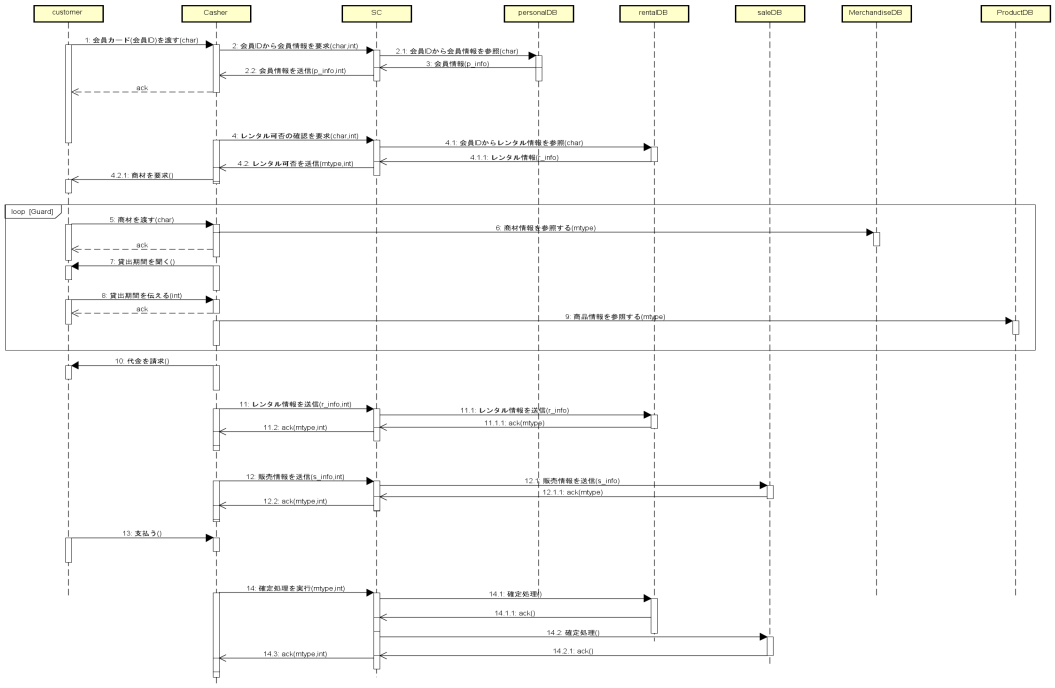

図 5　レンタルパターンのシーケンス図 (返却フェーズ)

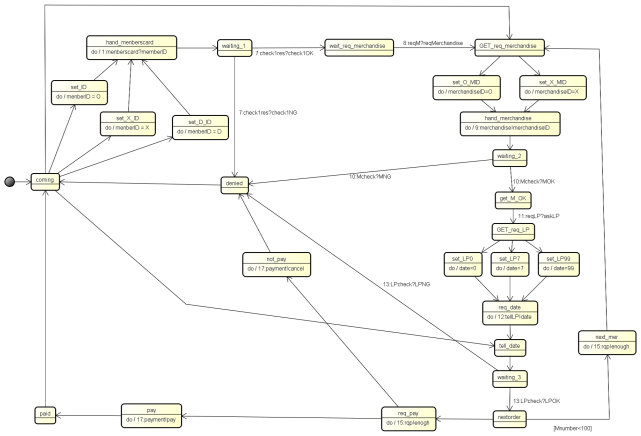

図 6　追加した顧客のステートマシン図

いことを示すために，作成したモデルに対して SPIN によるモデル検査を行う．SPIN によるモデル検査には PROMELA 記述が必要であるが，UML-PROMELA 変換器により記述コストの削減が可能である．現在変換器の仕様に即した形にコミュニケーション図，ステートマシン図の深化を行っている．今後は，顧客の振る舞い要素の追加など，さらなるモデルの深化を行い，モデル検査を行う．どの様な顧客に対しても停止しないことを検証した後に，作成した上位設計に沿ってプロトタイピングを行い，作成した上位設計全体の検査を実施する．

参考文献

[1] 後藤亮馬, 和崎克己 : “UML-PROMELA 変換器を用いた ZigBeeIP/RPL プロトコルにおけるノード探索仕様の検証” ; FIT2014（第 13 回情報科学技術フォーラム）講演論文集, (B-019), 159-162, 2014.
[2] 坂本統, 和崎克己 : “タイムアウト機構を有するメッセージ交換プロトコルの UML モデルと SPIN モデル検査” ; FIT2013（第 12 回情報科学技術フォーラム）講演論文集, (B-021), 267-270, 2013.
[3] UML Resource Page, The Unified Modeling Language(UML),the Object Management Group(OMG), http://www.uml.org/
[4] 株式会社チェンジビジョン, http://www.changevision.com/
[5] Gerard J. Holzmann : “The SPIN Model Checker” ; Addison-Wesley, 2004.
[6] 吉岡信和, 青木利晃, 田原康之 : “SPIN による設計モデル検証” ; 近代科学社, 2009.
[7] 中島震 : “SPIN モデル検査” ; 近代科学社, 2008.